

Beam-forming for Secure Communication in Amplify-and-Forward Networks: An SNR based approach

Siddhartha Sarma, Samar Agnihotri, and Joy Kuri

Abstract

The problem of secure communication in Amplify-and-Forward (AF) relay networks with multiple eavesdroppers is considered. Assuming that a receiver (destination or eavesdropper) can decode a message only if the received SNR is above a predefined threshold, we introduce SNR based optimization formulations to calculate optimal scaling factors for relay nodes in two scenarios. In the first scenario, we maximize the achievable rate at the legitimate destination, subject to the condition that the received SNR at each eavesdropper is below the target threshold. Due to the non-convex nature of the objective function and eavesdroppers' constraints, we transform variables and obtain a *Quadratically Constrained Quadratic Program* (QCQP) with convex constraints, which can be solved efficiently. When the constraints are not convex, we consider a *Semi-definite relaxation* (SDR). In the second scenario, we minimize the total power consumed by all relay nodes, subject to the condition that the received SNR at the legitimate destination is above the threshold and at every eavesdropper, it is below the corresponding threshold. We propose a *semi-definite relaxation* of the problem in this scenario and also provide an analytical lower bound.

I. INTRODUCTION

In wireless networks, generally security measures are implemented in the upper layers of protocol stack using cryptographic methods. However, current advances in computation technology pose threats for such systems, prompting researchers to explore alternatives like *physical layer security* [1]. In ad-hoc wireless networks, where relay nodes are constrained by hardware or available energy resources, physical-layer based schemes can indeed provide effective solutions.

In the physical-layer security literature, most results are centered around an information-theoretic measure - the *secrecy capacity* [2]. The secrecy capacity is the maximum rate of information transfer from the source to the destination in the presence of eavesdropper(s). However, even for many simple networks, calculating secrecy capacity for a given eavesdropper model is a tedious task as it involves solving fractional optimization problems, which are known to be NP-hard in general [3]. For amplify-and-forward (AF) relay networks, the authors in [4] evaluated secrecy capacity for a single eavesdropper, and the zero-forcing secrecy rate for multiple eavesdroppers under a total relay power constraint. In [5] and [6], techniques are devised for computing the maximum AF secrecy rate with a single and multiple eavesdroppers under both individual and total relay

S. Sarma and J. Kuri are with the Department of Electronic Systems Engineering, Indian Institute of Science, Bangalore, Karnataka - 560012, India (e-mail: {siddharth, kuri}@dese.iisc.ernet.in).

S. Agnihotri is with the School of Computing and Electrical Engineering, Indian Institute of Technology Mandi, Mandi, Himachal Pradesh - 175001, India (e-mail: samar@iitmandi.ac.in).

power constraints, respectively. However, our work differs from them as we have considered an SNR based model for secure communication. The motivation for our approach arises from the results in [7], where it is shown that the secrecy capacity depends on the source-destination and the source-eavesdropper channel capacities, which in turn are functions of the respective signal-to-noise ratios (SNR).

In practical receivers, the correct decoding of the received signals is dependent on the received SNR [8]. If the received SNR is below a certain predefined threshold, then for all practical purposes, we can assume that the receiver cannot extract any information from the received signal. Following this argument, we consider a model where every eavesdropper has limited decoding capability, determined by its SNR threshold. Therefore, to ensure secure communication between the source and the destination, we strive to bring down the received SNR at each eavesdropper below its target SNR threshold. This approach is a generalization of the zero-forcing approaches for secure communication [4]. Concurrently, we also strive to improve the SNR at the legitimate destination. This leads us to our first scenario, where we maximize the achievable rate at the legitimate destination, subject to the condition that the received SNR at each eavesdropper is below its target threshold. We address this scenario in Section III. Though a similar problem was considered in [6], but unlike them we are not interested in evaluating optimal secrecy rate. Infact, as each eavesdropper can have a different threshold, therefore the optimal solution of our problem will differ from the solution of *Secrecy Rate Maximization* (SRM) problem considered in [6]. Also, we propose a noble transformation for this problem to obtain a *Quadratic Constrained Quadratic Program* (QCQP) which attains global solution under certain criteria.

The second scenario that we consider is motivated by wireless adhoc networks, where the intermediate relay nodes may be interested in minimizing total power consumption while ensuring secure communication between the source and the destination. In such scenarios, we would like to minimize the total power consumption of relay nodes, subject to the condition that the received SNR at the legitimate destination is above a predefined threshold and at every eavesdropper it is below the respective predefined threshold. This formulation is described in Section IV.

A similar SNR based model is also considered in [9]. However, unlike the decode-and-forward (DF) relaying used in that work, we employ AF relaying as it is one of the simplest relaying schemes and even in low-SNR regimes, it can be a capacity achieving relay strategy in some scenarios [10].

II. SYSTEM MODEL

The system consists of a single source (S), a single destination (D), M relay nodes ($i \in \mathcal{M} = \{1, 2, \dots, M\}$) and K eavesdroppers ($k \in \mathcal{K} = \{1, 2, \dots, K\}$) as shown in Figure 1. The channel gain from a node p to a node q is denoted by a complex constant $h_{p,q}$, where $p \in \{S\} \cup \mathcal{M}$ and $q \in \{D\} \cup \mathcal{M} \cup \mathcal{K}$. We assume the availability of complete channel state information (CSI), *i.e.*, all $h_{p,q}$ values are known throughout the network [4], [9]. Considering discrete time instants and neglecting propagation delays, the signal received at each relay node due to the source can be expressed as:

$$y_i[n] = h_{s,i}x_s[n] + z_i[n] \quad (1)$$

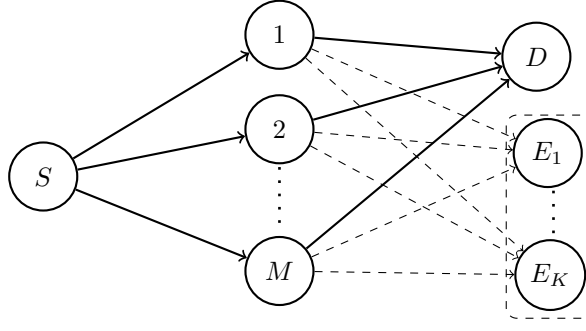


Fig. 1. Simple AF network with multiple ($K > 1$) eavesdroppers.

where the source signal $x_s[n]$ at time instant n , $-\infty < n < \infty$, are i.i.d complex Gaussian random variables with zero mean and variance P_s . Further, $x_s[n]$ is assumed to be independent of $z_i[n]$, the complex white Gaussian noise ($\sim \mathcal{CN}(0, \sigma^2)$) at the i^{th} relay node. Each relay node i scales the received signal from the source by $\beta_i \in \mathbb{C}$ before transmitting:

$$x_i[n+1] = \beta_i y_i[n], |\beta_i|^2 \leq \beta_{i,max}^2 = \frac{P_i}{|h_{s,i}|^2 P_s + \sigma^2} \quad (2)$$

where $\mathbf{E}[|x_i[n]|^2] \leq P_i$, $\forall i \in \mathcal{M}$. Therefore, the received signal at the destination or an eavesdropper can be expressed as:

$$y_l[n] = \sum_{i=1}^M h_{i,l} x_i[n] + z_l[n], l \in \{D\} \cup \mathcal{K} \quad (3)$$

Here $z_l[n] \sim \mathcal{CN}(0, \sigma^2)$. We assume that z_i are independent of the source symbol and of each other. For the layered relay network shown in Figure 1, the received signals at the destination and the eavesdroppers are free of intersymbol interference as they traverse paths with the same respective delays. Therefore, omitting the time index and using (1), (2) and (3) we can write:

$$y_l = \sum_{i=1}^M h_{s,i} \beta_i h_{i,l} x_s + \sum_{i=1}^M \beta_i h_{i,l} z_i + z_l \quad (4)$$

From (4), we can write the SNR at the destination or an eavesdropper as:

$$SNR_l = \frac{\left| \sum_{i=1}^M h_{s,i} \beta_i h_{i,l} \right|^2}{1 + \sum_{i=1}^M |\beta_i h_{i,l}|^2} \frac{P_s}{\sigma^2} = \frac{|\mathbf{h}_{s,l}^\dagger \boldsymbol{\beta}|^2}{1 + \boldsymbol{\beta}^\dagger \mathbf{D}_l \boldsymbol{\beta}} \frac{P_s}{\sigma^2}$$

where $\mathbf{h}_{s,l}$ is an $M \times 1$ column vector $\mathbf{h}_{s,l} = [h_{s,1}h_{1,l}, h_{s,2}h_{2,l}, \dots, h_{s,M}h_{M,l}]^\dagger$ and \mathbf{D}_l is a $M \times M$ diagonal matrix *i.e.*, $\mathbf{D}_l = \text{diag}(|h_{1,l}|^2, \dots, |h_{M,l}|^2)$, $l \in \{D\} \cup \mathcal{K}$.

III. RECEIVER SNR MAXIMIZATION

In the first scenario, we consider the problem of maximizing the secrecy rate achievable with the AF-relays when the received SNR at the eavesdroppers is below their respective predefined thresholds. However, given the logarithmic dependence of the achievable information rate on the received SNR ($I(P_s) \propto \log(1 + SNR)$) and the monotonically increasing nature of the

$\log(\cdot)$, we have:

$$\mathbf{P1:} \max_{\boldsymbol{\beta}} \frac{\left| \sum_{i=1}^M h_{s,i} \beta_i h_{i,d} \right|^2}{1 + \sum_{i=1}^M |\beta_i h_{i,d}|^2} \frac{P_s}{\sigma^2} \quad (5a)$$

$$\text{such that } \frac{\left| \sum_{i=1}^M h_{s,i} \beta_i h_{i,k} \right|^2}{1 + \sum_{i=1}^M |\beta_i h_{i,k}|^2} \frac{P_s}{\sigma^2} \leq \gamma_k, \quad k \in \mathcal{K} \quad (5b)$$

$$|\beta_i|^2 \leq \beta_{max,i}^2, \quad i \in \mathcal{M} \quad (5c)$$

Here, γ_k is a real number and represents the predefined threshold for the k^{th} eavesdropper. This problem is inherently non-convex. We consider the following transformation of the variable β_i .

$$\omega_i = \beta_i h_{i,d}, \text{ and } u_i = \frac{\omega_i}{\sqrt{1 + \boldsymbol{\omega}^\dagger \boldsymbol{\omega}}}$$

If we consider the vector variables $\mathbf{u} = [u_1, u_2, \dots, u_M]^\mathbf{t}$ and $\boldsymbol{\omega} = [\omega_1, \omega_2, \dots, \omega_M]^\mathbf{t}$, then we can write:

$$\mathbf{u} = \frac{\boldsymbol{\omega}}{\sqrt{1 + \boldsymbol{\omega}^\dagger \boldsymbol{\omega}}} \Leftrightarrow \boldsymbol{\omega} = \frac{\mathbf{u}}{\sqrt{1 - \mathbf{u}^\dagger \mathbf{u}}}$$

Also, we define $\boldsymbol{\rho}_k = [\rho_{1,k}, \dots, \rho_{M,k}]$, where $\rho_{i,k} = \frac{h_{i,k}}{h_{i,d}}$.

In terms of these new variables and parameters, the objective function and constraints are expressed in the following way:

- **Objective function:**

$$\frac{|\mathbf{h}_s^\dagger \boldsymbol{\omega}|^2}{1 + \boldsymbol{\omega}^\dagger \boldsymbol{\omega}} = |\mathbf{h}_s^\dagger \mathbf{u}|^2, \text{ where } \mathbf{h}_s = [h_{s,1}, \dots, h_{s,M}]^\dagger$$

- **Eavesdroppers Constraint $\forall k \in \mathcal{K}$:**

$$\begin{aligned} \mathbf{h}_{s\rho,k} &= [h_{s,1}\rho_{1,k}, h_{s,2}\rho_{2,k} \dots, h_{s,M}\rho_{M,k}]^\dagger \\ \frac{\left| \sum_{i=1}^M h_{s,i} \beta_i h_{i,k} \right|^2}{1 + \sum_{i=1}^M |\beta_i h_{i,k}|^2} &= \frac{\boldsymbol{\omega}^\dagger (\mathbf{h}_{s\rho,k} \mathbf{h}_{s\rho,k}^\dagger) \boldsymbol{\omega}}{1 + \boldsymbol{\omega}^\dagger \mathbf{D}_{\rho,k} \boldsymbol{\omega}} \leq \gamma'_k, \end{aligned}$$

where $\mathbf{D}_{\rho,k} = \text{diag}(\boldsymbol{\rho}_k)$ and $\gamma'_k = \gamma_k \frac{\sigma^2}{P_s}$, $\forall k \in \mathcal{K}$. By writing in terms of \mathbf{u} and rearranging, we get: $\mathbf{u}^\dagger \mathbf{C}_k \mathbf{u} \leq 1$, where

$$\mathbf{C}_k = \frac{\mathbf{h}_{s\rho,k} \mathbf{h}_{s\rho,k}^\dagger}{\gamma'_k} + \mathbf{I} - \mathbf{D}_{\rho,k}$$

- **Relay power constraint $\forall i \in \mathcal{M}$:**

$$\begin{aligned} |\beta_i|^2 &= \frac{|\omega_i|^2}{|h_{i,d}|^2} = \frac{|u_i|^2}{|h_{i,d}|^2 (1 - \mathbf{u}^\dagger \mathbf{u})} \leq \beta_{i,max}^2 \\ \text{or } \mathbf{u}^\dagger \mathbf{u} + \frac{|u_i|^2}{|h_{i,d}|^2 \beta_{i,max}^2} &\leq 1 \text{ or } \mathbf{u}^\dagger \mathbf{D}_i \mathbf{u} \leq 1, \end{aligned}$$

where

$$(\mathbf{D}_i)_{jk} = \begin{cases} 1 + \frac{1}{|h_{i,d}|^2 \beta_{i,max}^2}, & \text{if } k = j = i \\ 1, & \text{if } k = j \neq i \\ 0, & \text{otherwise} \end{cases}$$

Therefore, the equivalent optimization problem is:

$$\mathbf{P1-EQ:} \max_{\mathbf{u}} \mathbf{u}^\dagger \mathbf{h}_s \mathbf{h}_s^\dagger \mathbf{u} \quad (6a)$$

$$\text{such that } \mathbf{u}^\dagger \mathbf{C}_k \mathbf{u} \leq 1, \quad k \in \mathcal{K} \quad (6b)$$

$$\mathbf{u}^\dagger \mathbf{D}_i \mathbf{u} \leq 1, \quad i \in \mathcal{M} \quad (6c)$$

If $\rho_{i,k} = \frac{|h_{i,k}|}{|h_{i,d}|} \leq 1, \forall i, k$ then $\mathbf{I} - \mathbf{D}_{\rho,k}$ is a diagonal matrix with positive entries, therefore, \mathbf{C}_k is a positive definite matrix. As the objective function and all the constraints are convex, we can obtain the global optimum using numerical routines as suggested by [11].

But, in general scenarios \mathbf{C}_k may not be positive-semidefinite. However, if a **QCQP** is not convex then it is hard to solve [12], [13]. As $\mathbf{u}^\dagger \mathbf{h}_s \mathbf{h}_s^\dagger \mathbf{u} = \text{Trace}(\mathbf{u}^\dagger \mathbf{h}_s \mathbf{h}_s^\dagger \mathbf{u}) = \text{Trace}(\mathbf{h}_s \mathbf{h}_s^\dagger \mathbf{u} \mathbf{u}^\dagger)$, so by considering relaxation on rank one symmetric positive semi-definite (PSD) matrix $\mathbf{U} = \mathbf{u} \mathbf{u}^\dagger$, the optimization program 6 can be written as:

$$\max_{\mathbf{U}} \quad \mathbf{h}_s \mathbf{h}_s^\dagger \bullet \mathbf{U} \quad (7a)$$

$$\text{subject to} \quad \mathbf{C}_k \bullet \mathbf{U} \leq 1, \quad k \in \mathcal{K} \quad (7b)$$

$$\mathbf{D}_i \bullet \mathbf{U} \leq 1, \quad i \in \mathcal{M} \quad (7c)$$

The \bullet represents Frobenius product of matrices, $\mathbf{A} \bullet \mathbf{B} = \text{Trace}(\mathbf{A}^\dagger \mathbf{B})$. Once the problem 7 is solved, we can find the corresponding optimal \mathbf{u} and thereby \mathbf{w} by applying eigenvalue decomposition on matrix \mathbf{U} [13].

Remark 1: If we denote the optimum objective function value by SNR_d^* , then source can securely transmit at a rate $\frac{1}{2} \log(1 + \frac{\text{SNR}_d^*}{\text{SNR}_d^* - \gamma_d} [\text{SNR}_d^* - \gamma_d]^+)$, where $[x]^+ = \max\{x, 0\}$ and γ_d is the SNR threshold for destination.

IV. RELAY POWER MINIMIZATION

For an energy constrained relay network, an objective would be to minimize the total relay power. Using (2), the power of the signal transmitted by the i^{th} relay node is $|\beta_i|^2 (|h_{s,i}|^2 P_s + \sigma^2), \forall i \in \mathcal{M}$. Considering the SNR constraints on the destination and the eavesdroppers and individual power constraint for each relay node, the total relay power minimization problem is as follows:

$$\mathbf{P2:} \min_{\beta} \sum_{i=1}^M |\beta_i|^2 (|h_{s,i}|^2 P_s + \sigma^2) \quad (8a)$$

$$\text{such that } \frac{\left| \sum_{i=1}^M h_{s,i} \beta_i h_{i,d} \right|^2}{1 + \sum_{i=1}^M |\beta_i h_{i,d}|^2} \frac{P_s}{\sigma^2} \geq \gamma_d \quad (8b)$$

$$\frac{\left| \sum_{i=1}^M h_{s,i} \beta_i h_{i,k} \right|^2 P_s}{1 + \sum_{i=1}^M |\beta_i h_{i,k}|^2 \sigma^2} \leq \gamma_k, \quad k \in \mathcal{K} \quad (8c)$$

$$|\beta_i|^2 \leq \beta_{max,i}^2, \quad i \in \mathcal{M} \quad (8d)$$

Similar to γ_k , γ_d is a real number and it represents the predefined SNR threshold for the destination. We can easily rewrite the above expression in matrix notation and rearrange to get the following Quadratic Constrained Quadratic Program (QCQP) formulation [12]:

$$\begin{aligned} \mathbf{P2-QCQP:} \quad & \min_{\boldsymbol{\beta}} \quad \boldsymbol{\beta}^\dagger \mathbf{Q}_0 \boldsymbol{\beta} \\ & \boldsymbol{\beta}^\dagger \mathbf{Q}_D \boldsymbol{\beta} \geq \gamma'_d \\ & \boldsymbol{\beta}^\dagger \mathbf{Q}_k \boldsymbol{\beta} \leq \gamma'_k, \quad k \in \mathcal{K} \\ & |\beta_i|^2 \leq \beta_{max,i}^2, \quad i \in \mathcal{M} \end{aligned}$$

$$\text{where } \gamma'_l = \frac{\sigma^2}{P_s} \gamma_l, \quad l \in \{D\} \bigcup \mathcal{K}$$

$$\mathbf{Q}_0 = \text{diag}(|h_{s,1}|^2 P_s + \sigma^2, |h_{s,2}|^2 P_s + \sigma^2, \dots, |h_{s,M}|^2 P_s + \sigma^2)$$

$$\mathbf{Q}_l = \mathbf{h}_{s,1} \mathbf{h}_{s,1}^\dagger - \gamma'_l \mathbf{D}_l, \quad l \in \{D\} \bigcup \mathcal{K}$$

Following the procedures discussed in previous section, we formulate another semi-definite program after relaxing the symmetric positive semi-definite (PSD) matrix $\mathbf{B} = \boldsymbol{\beta} \boldsymbol{\beta}^\dagger$.

$$\mathbf{P2-SDR:} \quad \min_{\mathbf{B}} \quad \mathbf{Q}_0 \bullet \mathbf{B} \quad (9a)$$

$$-\mathbf{Q}_D \bullet \mathbf{B} \leq -\gamma'_d \quad (9b)$$

$$\mathbf{Q}_k \bullet \mathbf{B} \leq \gamma'_k, \quad k \in \mathcal{K} \quad (9c)$$

$$\mathbf{B}_i \leq \beta_{max,i}^2, \quad i \in \mathcal{M} \quad (9d)$$

$$\mathbf{B} \succeq 0 \quad (9e)$$

\mathbf{B}_i represents the i^{th} diagonal element of that matrix. Solving this will provide us \mathbf{B} ; we look for an eigenvector of \mathbf{B} corresponding to the maximum eigenvalue.

All the above formulations of Problem P2 require iterative algorithms to obtain the optimal solution. Therefore, we discuss a simple analytical relaxed solution for the problem (8).

Analytical Relaxed Solution: It can be argued that to minimize the objective function value, (8b) should be satisfied with equality. Therefore, we formulate another optimization problem to calculate the analytical relaxed solution of the original objective function value.

$$\min_{\boldsymbol{\beta}} \quad \boldsymbol{\beta}^\dagger \mathbf{Q}_0 \boldsymbol{\beta} \quad (10a)$$

$$\text{such that } \beta^\dagger \mathbf{Q}_D \beta = \gamma'_d \quad (10b)$$

This can be posed as the well known *Rayleigh Quotient* [14, p. 176] problem *i.e.*

$$\min_{\beta} \quad \gamma'_d \frac{\beta^\dagger \mathbf{Q}_0 \beta}{\beta^\dagger \mathbf{Q}_D \beta} \quad (11)$$

If \mathbf{Q}_D is invertible, then the solution to this optimization problem is given by $\gamma'_d \lambda_{\min}$, where λ_{\min} is the minimum eigenvalue of matrix $\mathbf{Q}_D^{-1} \mathbf{Q}_0$ and the optimal β is the corresponding eigenvector. The solution of this problem need not satisfy the eavesdroppers' constraints, but the objective function value serves as lower bound for optimization problem 9 and indicate the extra amount of power required to met the secrecy constraints.

Remark 2: A lower bound on the achievable AF secrecy rate for the optimum scaling vector would be $\frac{1}{2} \log(1 + \gamma_d)$.

V. RESULTS

In Figure 2, we plot the solution of the destination SNR maximization problem, mentioned in Section III, with respect to source power (P_s) for several values of eavesdroppers' SNR threshold ($\gamma_k = \gamma_e = \text{constant}$, $k \in \mathcal{K}$) after averaging over 100 network instances. For each instance, the channel gains are obtained from a complex Gaussian distribution with mean 0 and variance 1. We considered five relay nodes ($M = 5$) with equal maximum transmit power ($P_i = 10$, $i \in \mathcal{M}$) and five eavesdroppers ($K = 5$) for the evaluation. Though we have assumed equal threshold values (γ_e) for all the eavesdroppers in our plots, our formulations are valid for unequal values ($\gamma_i \neq \gamma_j$ where $i \neq j, i, j \in \mathcal{K}$) also. As γ_e increases, the relay nodes can transmit signals with higher power. This results in the increase of SNR at the destination, yet the received SNRs at the eavesdroppers remain below their respective SNR thresholds. This leads to an increase in the secure communication rate with increasing γ_e , which is evident from Figure 2.

Figure 3 depicts the variation of optimal total relay power consumption for the total relay power minimization formulations, mentioned in Section IV, with respect to the source power (P_s). The "SDR" and "Analytical Relaxed" values are outputs of the relaxed semidefinite program **P2-SDR** and Rayleigh Quotient problem (11), respectively. With the increase of source power (P_s), the SNR at relay nodes increases. Therefore, to maintain the SNR at the destination at any fixed value, the relays have to consume less power. This is apparent from Figure 3, which shows decreasing total relay power consumption with the increase of P_s .

VI. CONCLUSION

SNR based secure communication for Amplify-and-Forward (AF) relay networks with multiple eavesdroppers is considered. After motivating the secure communication scheme, we formulate two optimization problems for obtaining respective optimal scaling factors. Due to the non-convexity of both the formulations, we reformulate those for obtaining computationally efficient solutions. We have considered a two hop network, but in future we plan to investigate similar SNR based model for general multihop AF networks. We also plan to study scenarios where some relay nodes act as jammers, thereby reducing the SNR at the eavesdroppers [9], [15].

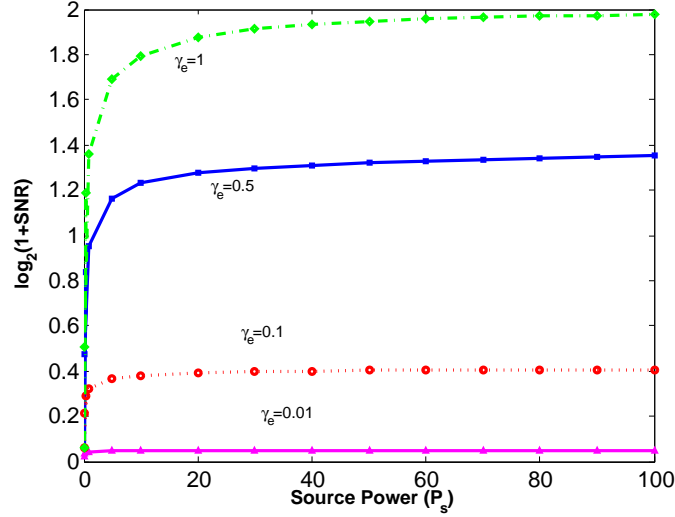


Fig. 2. Plot of the achievable secrecy rate at the destination $\log_2(1 + SNR_d)$ obtained from SNR maximization problem (P1) w.r.t. to source power (P_s) for several SNR threshold values (γ_e) with $P_i = 10$, $\sigma^2 = 1$, $M = 5$ and $K = 5$, averaged over 100 instances.

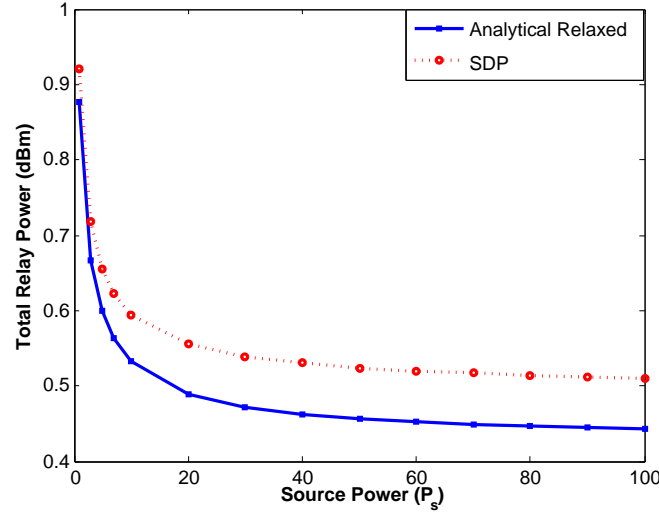


Fig. 3. Plot of total relay power consumption calculated using optimization formulations in (8),(9), and (11) w.r.t source power (P_s) with $\gamma_d = 0.01$ and $\gamma_e = 0.005$, $P_i = 10$, $\sigma^2 = 1$, $M = 5$ and $K = 5$, averaged over 100 instances.

REFERENCES

- [1] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, 2011.
- [2] A. Wyner, "The Wire-tap channel," *Bell Sys. Tech. Journal*, vol. 54, no. 8, pp. 1355–1387, Jan 1975.
- [3] S. Schaible and J. Shi, "Fractional programming: the sum-of-ratios case", *Optimization Methods and Software*, vol. 18, April 2003.
- [4] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," *Proc. IEEE ICASSP 2009*, Taipei, Taiwan, April 2009.
- [5] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secrecy," *Proc. IEEE ICC 2010*, Cape Town, South Africa, May 2010.
- [6] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. Ching, "Cooperative Secure Beamforming for AF Relay Networks With Multiple Eavesdroppers," *IEEE Signal Processing Letters*, vol. 20, no. 1, pp. 35–38, 2013.
- [7] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Info. Theory*, vol. IT-24, no. 4, pp. 451–456, July 1978.
- [8] J. G. Proakis, *Digital communications*, McGraw-Hill, New York, 1995.
- [9] S. Sarma, S. Shukla, and J. Kuri, "Joint scheduling & jamming for data secrecy in wireless networks," *Proc. IEEE WiOpt 2013*, Tsukuba, Japan, May 2013.
- [10] K. S. Gomadam and S. A. Jafar, "Optimal relay functionality for SNR maximization in memoryless relay networks," *IEEE JSAC*, vol. 25, February 2007.

- [11] J.-B. Hiriart-Urruty, “Global Optimality Conditions in Maximizing a Convex Quadratic Function Under Convex Quadratic Constraints,” *Journal of Global Optimization*, vol. 21, no. 4, pp. 443–453, 2001.
- [12] A. Qualizza, P. Belotti, and F. Margot, “Linear Programming Relaxations of Quadratically Constrained Quadratic Programs,” in *Mixed Integer Nonlinear Programming*, ser. The IMA Volumes in Mathematics and its Applications, J. Lee and S. Leyffer, Eds. Springer New York, 2012, vol. 154, pp. 407–426.
- [13] Z.-Q. Luo, W.-K. Ma, A.-C. So, Y. Ye, and S. Zhang, “Semidefinite relaxation of quadratic optimization problems,” *IEEE Sig. Process. Mag.*, vol. 27, no. 3, pp. 20–34, 2010.
- [14] R. A. Horn and C. R. Johnson, Eds., *Matrix Analysis*. New York, NY, USA: Cambridge University Press, 1986.
- [15] S. Sankararaman, K. Abu-Affash, A. Efrat, S. D. Eriksson-Bique, V. Polishchuk, S. Ramasubramanian, and M. Segal, “Optimization schemes for protective jamming,” *Proc. ACM Mobihoc 2012*, Hilton Head Island, SC, June 2012.